IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA

v.

ALEKSANDR RYZHENKOV
a/k/a Aleksandr Viktorovi3 Ryjenkov
a/k/a Aleksandr Viktorovich Ryzhenkov
a/k/a Aleksan Ryzhenkov
a/k/a Mrakobek
a/k/a Lizardking
a/k/a J.d.m0rris0n
a/k/a Jim Morrison
a/k/a G
a/k/a Guester
a/k/a Kotosel
a/k/a Anonyminem

NO. 3-23CR0098-F

FILED UNDER SEAL

INDICTMENT

The Grand Jury charges:

At all times material to this indictment:

General Allegations

1. "Malware" is a malicious software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, and do other unauthorized action on a computer system. Common examples of malware include viruses, ransomware, worms, keyloggers, and spyware.

2. "Ransomware" is a type of malware that infects a computer and encrypts some or all of the data on the computer. Distributors of ransomware typically extort the user of the encrypted computer by demanding that the user pay a ransom in order to decrypt and recover the data on the computer.

3. "BitPaymer" is a form of ransomware that encrypts victim computers. BitPaymer has been given other names by security researchers, such as FriedEx and iEncrypt.

4. "Bitcoin" is a type of virtual currency, circulated over the Internet as a form of value. Bitcoin are not issued by any government, bank, or company, but they are generated and controlled through computer software operating via a decentralized, peer-to-peer network. To acquire Bitcoin, typically a user will purchase them from a Bitcoin seller or "exchanger."

5. "Bitcoin addresses" are particular locations to which Bitcoin are sent and received. A Bitcoin address is analogous to a bank account number and is represented as a 26-to-35 character-long, case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key which is a cryptographic equivalent of a password and is needed to access the Bitcoin address. Only the holder of a Bitcoin address's private key can authorize a transfer of Bitcoin from that address to another Bitcoin address. Little to no personally identifiable information about a Bitcoin account holder is transmitted during a Bitcoin transaction.

6. A "command and control server" is a centralized computer that issues commands to remotely connected computers. "Command and Control" ("C2") infrastructure consists of servers and other technical infrastructure that issues commands to control malware.

7. Computer programs, including malware, are written in computer programing languages which include JavaScript and PowerShell.

8. "Dridex" is a malware specifically crafted to defeat antivirus and other protective measures employed by computer owners. Dridex is generally distributed through a process known as "phishing" where spam emails are distributed to recipients. The emails appear legitimate and are crafted to entice the recipient to click on a hyperlink or open an attached file. By clicking on the hyperlink or opening the attached file, the malware is installed onto the recipient's computer without the recipient's consent and knowledge.

9. "Drive-by-downloads" are downloads which a user has authorized, but without full understanding of the consequences (e.g., downloads which install an unknown program, counterfeit executable program, or a computer virus).

10. "Encryption" is the translation of data into a secret code. In order to access encrypted data, a user must have access to a password, commonly referred to as a "decryption key" or "decryptor" that enables the user to decrypt the data.

11. A "loader" is a term used for a basic remote access trojan (i.e., malware disguised as legitimate software). The loader is designed to install additional malware components onto a victim computer and to evade detection of antivirus programs. Dridex can be used as a loader.

12. "Security vulnerabilities" are unintended flaws in software code or an operating system that leaves a computer open to exploitation in the form of unauthorized access and malicious behavior (e.g., the deployment of malware).

13. "Tether" is a type of virtual currency, circulated over the Internet as a form of value.

14. Tor is a computer network designed to facilitate anonymous communication over the Internet. The Tor network does this by routing a user's communications through a globally distributed network of relay computers in a manner that renders ineffective any conventional Internet Protocol ("IP")-based methods of identifying users. The Tor network also enables users to operate hidden sites that operate similarly to conventional websites.

15. Company A was headquartered in Orange, Texas.

16. Company B was headquartered in Indianapolis, Indiana, and it had offices across North America and in Europe. Company B had a datacenter in Dallas, Texas, which was located in the Northern District of Texas.

17. Company C was headquartered in Lewisville, Texas.

18. Company D was headquartered in Dallas, Texas, which was located in the Northern District of Texas.

19. Company D was headquartered in Dallas, Texas, which was located in the Northern District of Texas.

20. Company E was headquartered in Dallas, Texas, which was located in the Northern District of Texas.

21. Defendant **Aleksandr Ryzhenkov** was a Russian citizen. **Ryzhenkov** used various online monikers including Mrakobek, Lizardking, J.d.m0rris0n, Jim Morrison, G, Guester, Kotosel, and Anonyminem.

Count One

Conspiracy to Commit Fraud and Related Activity in Connection with Computers
[Violation of 18 U.S.C. §§ 371 (18 U.S.C. §§ 1030(a)(5)(A) and 1030(a)(7)(C))]

22. Paragraphs 1 through 21 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

23. From on or about June 1, 2017, through on or about April 6, 2021, in the Northern District of Texas and elsewhere, defendant **Aleksandr Ryzhenkov** did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury, to commit an offense against the United States, that is,

a. to knowingly cause the transmission of a program, information, code, and command and as a result of such conduct, intentionally caused damage without authorization to a protected computer, and cause loss to persons during a 1-year period from the defendants' course of conduct affecting protected computers aggregating at least $5,000 in value, and caused damage affecting 10 or more protected computers during a 1-year period, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B); and

b. to knowingly and with intent to extort from any person any money and other thing of value, transmit in interstate and foreign commerce any communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, which such damage was caused to facilitate the extortion, in violation of 18 U.S.C. §§ 1030(a)(7)(C) and (c)(3)(A).

Purpose of the Conspiracy

24. It was the purpose of the conspiracy for defendant **Aleksandr Ryzhenkov** and other coconspirators to unlawfully enrich themselves and others by: (a) authoring BitPaymer ransomware that would, when executed, encrypt data on victims' computers; (b) conducting reconnaissance and research in order to target potential victims; (c) accessing victims' computers without authorization through security vulnerabilities; (d) installing and executing BitPaymer ransomware on victims' computers, resulting in the encryption of data on the computers; (e) extorting victims by demanding a ransom paid in Bitcoin in exchange for decryption keys to decrypt the data; and (f) collecting ransom payments from victims who paid the ransom.

Manner and Means of the Conspiracy

25. The manner and means by which defendant **Aleksandr Ryzhenkov** and other coconspirators sought to accomplish the purpose of the conspiracy included, among other things:

a. Unknown conspirators authored various versions of BitPaymer ransomware, which was designed to encrypt data on victims' computers. Conspirators deployed the first operational version of BitPaymer ransomware in or about July 2017. Since then, conspirators regularly have updated BitPaymer ransomware and refined the manner in which BitPaymer attacks are conducted.

b. Conspirators initially infected victims' computers in various ways, including by deploying phishing emails and facilitating drive-by-downloads containing malicious JavaScript and PowerShell code, and by using compromised

remote desktop credentials. The malicious code then downloaded Dridex and other loaders to the victims' computers to permit persistent remote access for the conspirators to the compromised computers.

c. Through this persistent remote access, the conspirators then used malware, including types named Powershell Empire and Mimikatz, as well as built-in software command line (i.e., text-based user interface) tools, to gain further access and control of other computers in the victims' networks in order to elevate access to administrator privileges on the victims' networks.

d. After gaining sufficient privileges and access to the computers in the victims' networks, the conspirators located backups and attempted to delete and encrypt the backups. Thereafter, the conspirators deployed BitPaymer ransomware on the victims' networks.

e. By the conspirators deploying BitPaymer ransomware, the files on the victims' computers were encrypted. Further, through the deployment of BitPaymer ransomware, the conspirators left an electronic note in the form of a text file on the victims' computers. The note included instructions on how to contact the conspirators to pay the ransom in order to have the victims' files decrypted.

f. Using the instructions left in the text file on the victims' computers, the victims then contacted the conspirators in various ways, such as email and the Tor network.

g. During the communications, the conspirators provided the ransom amount and the Bitcoin address where the ransom payment could be paid. At times, during the course of the communications, conspirators negotiated the ransom amount with the victims and the victims' representatives.

h. In the event a victim paid the ransom amount, conspirators provided the decryption key to the victims, and the victims then were able to access their files.

Overt Acts

26. In furtherance of the conspiracy and to affect its unlawful objects, the defendant, **Aleksandr Ryzhenkov**, and other coconspirators committed and caused to be committed the following overt acts in the Northern District of Texas and elsewhere:

a. On or about July 4, 2017, defendant **Aleksandr Ryzhenkov** searched online for information on various Bitcoin ransom amounts, ransomware hacks for a million dollars, and visited websites discussing ransomware attacks.

b. On or about July 26, 2017, defendant **Aleksandr Ryzhenkov** searched online for how to delete certain computer backups.

c. On or about July 29, 2017, conspirators accessed the internal computer networks of Company A without authorization and deployed BitPaymer ransomware, thereby encrypting Company A's computers.

d. On or about July 29, 2017, conspirators transmitted in interstate and foreign commerce a ransom demand in relation to encrypting Company A's computers, demanding an amount in exchange for a decryptor key to decrypt the data.

e. On or about July 30, 2017, defendant **Aleksandr Ryzhenkov** searched online for the following: Company A; how to gather user domains for computer networks; and computer tools and software such as PowerShell Empire.

f. On or about August 3, 2017, defendant **Aleksandr Ryzhenkov** and coconspirators exchanged electronic communications discussing hacking, encrypting, ransom amounts, and providing a decryptor key for multiple victim companies.

g. On or about September 7, 2017, defendant **Aleksandr Ryzhenkov** and a coconspirator exchanged electronic communications wherein **Ryzhenkov** offered to teach the coconspirator how to make money working for **Ryzhenkov** by hacking into computer networks, deploying encryption on computer networks, cashing out ransom demands in Bitcoin, and removing backups so backups cannot be restored.

h. On or about September 7, 2017, defendant **Aleksandr Ryzhenkov** also taught the coconspirator how to install Tor and setup a Powershell Empire C2 server.

i. On or about September 7, 2017, defendant **Aleksandr Ryzhenkov** and the coconspirator referenced in paragraphs 27.g and 27.h exchanged electronic communications wherein **Ryzhenkov** informed the coconspirator that two days earlier he had accessed without authorization two computer networks, and that one company paid a $35,000 ransom.

j. From on or about October 24, 2017, through on or about November 3, 2017, defendant **Aleksandr Ryzhenkov** and a coconspirator exchanged electronic communications discussing internal access to victims' computers; financial records of victim companies; and setting ransom amounts for multiple victims.

k. On or about January 12, 2018, defendant **Aleksandr Ryzhenkov** provided a coconspirator with information about Company B's computer system, including internal hostnames and internal file paths.

l. Between on or about January 14, 2018, and on or about January 18, 2018, conspirators accessed the internal computer networks of Company B, within the Northern District of Texas, without authorization and deployed BitPaymer ransomware thereby encrypting Company B's computers.

m. On or about January 14, 2018, conspirators transmitted in interstate and foreign commerce a ransom demand in relation to encrypting Company B's computers—demanding approximately $2,000,000 in Bitcoin in exchange for a decryptor key to decrypt the data.

n. On or about February 8, 2018, conspirators provided Company B with a decryptor key after receiving a total of approximately $500,000, in the form of Bitcoin, from Company B.

o. Beginning in or about July 2018 through in or about August 2018, a BitPaymer conspirator, who worked as a money mule in the conspiracy, caused four Bitcoin transactions totaling approximately $58,000 to be made, sending the Bitcoin to a coconspirator known to the Grand Jury.

p. On or about December 15, 2018, conspirators accessed the internal computer networks of Company C without authorization and deployed BitPaymer ransomware thereby encrypting Company C's computers.

q. On or about December 15, 2018, conspirators transmitted a ransom demand in relation to encrypting Company C's computers—demanding approximately $1,400,000, in the form of Bitcoin, in exchange for a decryptor key to decrypt the data.

r. On or about December 18, 2018, conspirators accessed the internal computer networks of Company D, within the Northern District of Texas, without authorization and deployed BitPaymer ransomware thereby encrypting Company D's computers.

s. On or about December 18, 2018, conspirators transmitted in interstate and foreign commerce a ransom demand in relation to encrypting Company D's computers—demanding approximately $950,000, in the form of Bitcoin, in exchange for a decryptor key to decrypt the data.

t. On or about December 19, 2018, conspirators provided Company D with a decryptor key after receiving a total of approximately $960,000, in the form of Bitcoin, from Company D.

u. On or about June 5, 2019, conspirators accessed the internal computer networks of Company E, within the Northern District of Texas, without authorization and deployed BitPaymer ransomware thereby encrypting Company E's computers.

v. On or about June 6, 2019, conspirators transmitted in interstate and foreign commerce a ransom demand in relation to encrypting Company E's computers demanding approximately $1,600,000, in the form of Bitcoin, in exchange for a decryptor key to decrypt the data.

w. On or about June 7, 2019, conspirators provided Company E with a decryptor key after receiving approximately $1,606,857, in the form of Bitcoin, from Company E.

All in violation of 18 U.S.C. § 371 (18 U.S.C. §§ 1030(a)(5)(A) and 1030(a)(7)(C)).

Counts Two through Four
Intentional Damage to a Protected Computer
[Violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B), and 2]

27. Paragraphs 1 through 21 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

28. On or about the dates set forth below, in the Northern District of Texas, and elsewhere, defendant **Aleksandr Ryzhenkov**, and others, did knowingly cause the transmission of a program, information, code, and command and, as a result of such conduct, intentionally caused damage, and attempted to cause damage, without authorization, to a protected computer, and the offense caused loss to persons during a 1-year period from the defendants' course of conduct affecting protected computers aggregating at least $5,000 in value, and caused damage affecting 1 or more protected computers during a 1-year period, described below for each count, each transmission consisting a sperate count:

Count	Date(s)	Victim
Two	January 14, 2018, through January 18, 2018	Company B
Three	December 18, 2018	Company D
Four	June 5, 2019	Company E

In violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B), and 2.

Counts Five and Six
Transmitting a Demand in Relation to Damaging a Protected Computer
[Violation of 18 U.S.C. §§ 1030(a)(7)(C) and (c)(3)(A), and 2]

29. Paragraphs 1 through 21 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

30. On or about the dates set forth below, in the Northern District of Texas and elsewhere, defendant **Aleksandr Ryzhenkov**, aided and abetted by others, with the intent to extort from persons money and other things of value, transmitted in interstate and foreign commerce a communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, described below for each count, each transmission constituting a separate count:

Count	Date	Victim	Approximate Ransom Demand in U.S. Dollars
Five	December 18, 2018	Company D	$926,000
Six	June 6, 2019	Company E	$1,600,000

In violation of 18 U.S.C. §§ 1030(a)(7)(C) and (c)(3)(A) and 2.

Count Seven
Conspiracy to Commit Money Laundering
[Violation of 18 U.S.C. §§ 1956(h) and 1956(a)(2)(A)]

31. Paragraphs 1 through 21 of this indictment are re-alleged and incorporated by reference as though fully set forth herein.

32. From on or about June 1, 2017, through on or about April 6, 2021, in the Northern District of Texas and elsewhere, defendant **Aleksandr Ryzhenkov** did knowingly combine, conspire, confederate, and agree with other persons known and unknown to the Grand Jury, to transport, transmit, and transfer, and attempt to transport, transmit, and transfer monetary instruments and funds from a place in the United States, to or through a place outside the United States, with the intent to promote the carrying on of a specified unlawful activity, that is, fraud and related activity in connection with computers, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (a)(7)(C).

All in violation of 18 U.S.C. §§ 1956(h) and 1956(a)(2)(A).

Forfeiture Notice
[18 U.S.C. §§ 982(a)(2)(B), 1030(i), and 982(a)(1)]

33. Paragraphs 1 through 32 of this indictment are realleged and incorporated by reference as though fully set forth herein.

34. Upon conviction for the offense alleged in Count One of this indictment, the defendant, **Aleksandr Ryzhenkov**, shall forfeit to the United States of America, pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of the violation.

35. Upon conviction for any of the offenses alleged in Counts Two through Six of this indictment, the defendant, **Aleksandr Ryzhenkov**, shall forfeit to the United States of America, pursuant to 18 U.S.C. § 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of the respective violation, and any property, real or personal, constituting or derived from, any proceeds obtained, directly or indirectly, as a result of the respective violation.

36. Upon conviction for the offense alleged in Count Seven of this indictment, the defendant, **Aleksandr Ryzhenkov**, shall forfeit to the United States of America, pursuant to 18 U.S.C. §§ 982(a)(1), any property, real or personal, involved in the offense, and any property traceable to that property.

37. Additionally, the forfeiture may consist of a forfeiture "money" judgment against the defendant convicted of the offense. Further, if any of the property described above, as a result of any act or omission of a defendant, cannot be located upon the exercise of due diligence; has been transferred or sold to, or deposited with, a third party; has been placed beyond the jurisdiction of the court; has been substantially diminished in

value; or has been commingled with other property which cannot be divided without difficulty, the United States of America shall be entitled to forfeiture of substitute property pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b)(1) and 28 U.S.C. § 2461(c).

A TRUE BILL

FOREPERSON

LEIGHA SIMONTON
UNITED STATES ATTORNEY

ERRIN MARTIN
Assistant United States Attorney
Texas Bar No. 24032572
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: 214-659-8600
Facsimile: 214-659-8805
Email: Errin.Martin@usdoj.gov

JOSEPH A. MAGLIOLO
Assistant United States Attorney
Texas Bar No. 24074634
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: 214-659-8600
Facsimile: 214-659-8805
Email: Joseph.Magliolo@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

THE UNITED STATES OF AMERICA

v.

ALEKSANDR RYZHENKOV
a/k/a Aleksandr Viktorovi3 Ryjenkov
a/k/a Aleksandr Viktorovich Ryzhenkov
a/k/a Aleksan Ryzhenkov
a/k/a Mrakobek
a/k/a Lizardking
a/k/a J.d.m0rris0n
a/k/a Jim Morrison
a/k/a G
a/k/a Guester
a/k/a Kotosel
a/k/a Anonyminem

SEALED INDICTMENT

18 U.S.C. §§ 371 (18 U.S.C. §§ 1030(a)(5)(A) and 1030(a)(7)(C))
Conspiracy to Commit Fraud and Related Activity in Connection with Computers
(Count 1)

18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B), and 2
Intentional Damage to a Protected Computer
(Counts 2 – 4)

18 U.S.C. §§ 1030(a)(7)(C) and (c)(3)(A), and 2
Transmitting a Demand in Relation to Damaging a Protected Computer
(Count 5 – 6)

18 U.S.C. §§ 1956(h) and 1956(a)(2)(A)
Conspiracy to Commit Money Laundering
(Count 7)

7 Counts

18 U.S.C. §§ 982(a)(2)(B), 1030(i), and 982(a)(1)
Forfeiture Notice

A true bill rendered

DALLAS FOREPERSON

Filed in open court this 21 day of March, 2023.

Warrant to be Issued

UNITED STATES MAGISTRATE JUDGE
No Criminal Matter Pending